



Secure BIOS

Publication number: CN1231787
Publication date: 1999-10-13
Inventor: DAVIS D L (US)
Applicant: INTEL CORP (US)
Classification:
- **international:** **G06F21/00; G06F21/00; (IPC1-7): H04K1/00**
- **european:** G06F21/00N3P1; G06F21/00N3P2
Application number: CN19971098335 19970730
Priority number(s): US19960724176 19960930

Also published as:

 WO9815082 (A1)
 EP0932953 (A1)
 US5844986 (A1)
 EP0932953 (A0)
 BR9711567 (A)

more >>

Report a data error here

Abstract not available for CN1231787

Abstract of corresponding document: **US5844986**

A subsystem prevents unauthorized modification of BIOS program code embedded in modifiable non-volatile memory devices such as flash memory. A cryptographic coprocessor containing the BIOS memory device performs authentication and validation on the BIOS upgrade based on a public/private key protocol. The authentication is performed by verifying the digital signature embedded in the BIOS upgrade.

Data supplied from the **esp@cenet** database - Worldwide